

KEYON

COMMUNICATIONS

February 28, 2008

Via ECFS

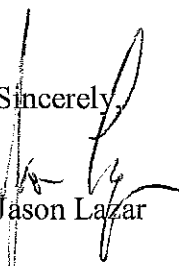
Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, SW
Washington, DC 20554

Re: CPNI Certification and Accompanying Statement
EB docket No. 06-36

Dear Ms. Dortch:

Keyon Communications Holdings, Inc., by its attorneys and pursuant to Section 64.2009(e) of the Commission's Rules, hereby submits its CPNI certification and accompanying statement.

Should you have any question or need further information, please contact the undersigned.

Sincerely,

Jason Lazar

cc: Telecommunications Consumers Division, Enforcement Bureau
Best Copy and Printing, Inc.

4061 Dean Martin Drive
Las Vegas, NV 89103
(702) 949-3580

KeyOn Communications Holdings, Inc.
SECTION 64.2009(E) CERTIFICATION
EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for the year 2007.

Date filed: February 29, 2008

Name of company covered by this certification: KeyOn Communications Holdings, Inc.

Form 499 Filer ID:

Name of signatory: Jason A. Lazar

Title of signatory: Vice President of Corporate Development and General Counsel

I, Jason A. Lazar, a duly authorized officer of KeyOn Communications Holdings, Inc., ("KeyOn") hereby certify on behalf of KeyOn, that I have personal knowledge that KeyOn has established operating procedures that are adequate to ensure compliance with the rules of the Federal Communications Commission, codified at 47 C.F.R. Part 64 Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken any actions against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.



Jason A. Lazar
VP of Corporate Development and General Counsel
KeyOn Communications Holdings, Inc.
February 29, 2008

**STATEMENT REGARDING OPERATING PROCEDURES
IMPLEMENTING 47 C.F.R. PART 64 SUBPART U
GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)
MARCH 1, 2008**

The following statement explains how the operating procedures of KeyOn Communications Holdings, Inc. ("KeyOn") and its subsidiaries ensure that it is in compliance with the Commission's CPNI rules, as codified at 47 C.F.R. Part 64 Subpart U and is relevant to calendar year 2007. Except as otherwise indicated, the following applies with respect to the Commission's rules in effect both before and after the December 8, 2007 effective date of the Commission's April 2, 2007 Report and Order in CC Docket No. 96-115. *See* FCC 07-22 (rel. Apr. 2, 2007); Public Notice, DA 07-4915 (rel. Dec. 6, 2007). This statement covers calendar year 2007.

Usage Statement

KeyOn has chosen to prohibit the use of CPNI for marketing and sales purposes by itself and between its subsidiaries.

KeyOn's CPNI Policy Manual includes an explanation of what CPNI is and when it may be used without customer approval.

Employees with access to CPNI, a narrow subset of KeyOn employees, have been trained as to when they are and are not authorized to use CPNI. The Company's CPNI Policy Manual describes the disciplinary process related to non-compliance with CPNI obligations and sets forth the penalties, including termination of employment.

The Company has established a review process regarding compliance with the FCC's CPNI rules.

The Company requires affirmative written/electronic subscriber approval for the release of CPNI to third parties. Electronic approval is documented through a notation in the customer's account information accessed through KeyOn's OSS.

A Corporate Officer is held responsible for annually certifying that KeyOn is in compliance with the FCC's CPNI rules and submitting the certification and accompanying statement explaining such, prior to March 1, 2008.

Company Safeguards

KeyOn takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. KeyOn also has safeguards in place to protect against the unauthorized access to CPNI such as having only a specific subset of employees who are able to access the information from our third-party partner. KeyOn authenticates a customer prior to disclosing CPNI based upon a customer-initiated telephone contact.

KeyOn only discloses call detail information over the telephone, based upon customer-initiated telephone contact, if the customer provides specific account information. If the customer can not provide certain account information, KeyOn only discloses call detail information by sending it to an address of record or by calling the customer at the telephone number of record. If the customer is able to provide call detail information during a customer-initiated call without KeyOn's assistance, then KeyOn is permitted to discuss the call detail information provided by the customer.

KeyOn has established a system of passwords and password protection.

For new customers, those that initiate service after the effective date of the CPNI rules, KeyOn requests that the customers establish a password at the time of initiation. For existing customers to create a password, KeyOn must first authenticate the customer with the use of readily available biographical information or account information. For example, KeyOn authenticates a customer using non-public information such as calling the customer at the telephone number of record.

A customer may access call detail information by establishing an online account by calling KeyOn's customer contact center and utilizing notations to KeyOn's OSS. If a password is forgotten or lost, KeyOn uses a back-up customer authentication method that is not based on readily available biographical or account information.

If a customer does not want to establish a password, the customer may still access call detail based on a customer-initiated telephone call, by asking KeyOn to send the call detail record to an address of record or by KeyOn calling the telephone of record.

KeyOn password-protects online access to all CPNI.

KeyOn has procedures and policies in place to notify a customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account or address or record is created or changed.

In the event of a CPNI breach, KeyOn complies with the FCC's rules regarding notice to law enforcement and customers. KeyOn maintains records of any discovered breaches and notifications to the United States Secret Service (USSS) and the FBI regarding those breaches, as well as the USSS and FBI responses to the notifications for a period of at least two years.

Actions Taken Against Data Brokers and Customer Complaints

KeyOn has taken no actions against data brokers in the last year. KeyOn has received no customer complaints in the past year concerning the unauthorized release of CPNI.